

# Mysteries of the World

# Stonehenge



# The Loch Ness Monster



# The Pyramids



# Grilled-Cheese Mary





# Crop Circles



# NASA's Software Engineering Standard





≡ Goddard Space Flight Center

# Demystifying the Rigors of Engineering Critical Software Systems

Isaac McGinnis/320.1

Manuel Maldonado/580



# Agenda

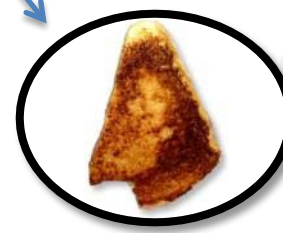
≡ Goddard Space Flight Center

What is  
NPR 7150.2A?



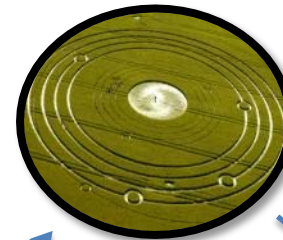
Classification/  
Inventory Process

Safety Criticality



Compliance

Final Thoughts



Q&A

# What is NPR 7150.2A





# What is NPR 7150.2



≡ Goddard Space Flight Center

---

- Documents NASA Best Practices
- CMMI Influence
- General Breakdown
  - Software Management Requirements
  - Software Engineering Process Requirements
  - Software Documentation and Work Product Requirements



# Process Management and Risk



≡ Goddard Space Flight Center

“A goal without a plan is just a wish.”  
- Antoine de Saint Exupery

## **7150 Translation**

The project shall:

- Develop software plan(s). [SWE-013]
- Peer reviews software plans [SWE-137], [SWE-087]:
- Maintain, and execute the software plan(s). [SWE-014]
- Track software activities against the software plans. [SWE-024]
- Ensure that changes to software plans are agreed to [SWE-026]
- Record and manage corrective actions for deviations from software plans [SWE-025]





# Process Management and Risk



≡ Goddard Space Flight Center

“If you cannot measure it, you cannot improve it.”  
- Lord Kelvin

## **7150 Translation**

- The Project shall provide software metric data per the Software Metrics Report. [SWE-044]
- The Software Metrics Report shall contain as a minimum the following information tracked on a CSCI basis: [SWE-117]
  - a. Software progress tracking measures.
  - b. Software functionality measures.
  - c. Software quality measures.
  - d. Software requirement volatility.
  - e. Software characteristics.



# Process Management and Risk



≡ Goddard Space Flight Center

“The devil is in the details.”  
- anonymous

## 7150 Translation

The project shall:

- Maintain a software cost estimate and associated cost parameter(s) that covers the **entire** software life cycle [SWE-015]
- Maintain a software schedule that coordinates with the overall project schedule, and documents the interactions of milestones and deliverables between software, hardware, operations, and the rest of the system [SWE-016]

**\*\*Chapter 5: Software Documentation Requirements – Provides the details of the content requirements for software plans and work products**



# Process Management and Risk



≡ Goddard Space Flight Center

“Traceability Rocks!”

- Someone very passionate about traceability

## 7150 Translation

The project shall:

- Maintain bidirectional traceability between the software requirement and the higher-level requirement. [SWE-052]
- Maintain bidirectional traceability between requirements and design. [SWE-059]
- Maintain bidirectional traceability from software design to code. [SWE-064]
- Maintain bidirectional traceability from the Software Test Procedures to the software requirements. [SWE-072]



# The Cliff Notes



≡ Goddard Space Flight Center

|                                                |                                                                                                                                                                                                                                                                                                     |                        |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Re                                             | For Class B software, If your organization has not been appraised/rated at CMMi level 2, a gap analysis is required                                                                                                                                                                                 | , 7123.1A              |
| So                                             |                                                                                                                                                                                                                                                                                                     | R)                     |
| So                                             |                                                                                                                                                                                                                                                                                                     | s Review (SRR)         |
| So                                             |                                                                                                                                                                                                                                                                                                     | review (PDR)           |
| So                                             | Per NPR 7150.2A [SWE-032]                                                                                                                                                                                                                                                                           | w (CDR)                |
| So                                             |                                                                                                                                                                                                                                                                                                     | ew (TRR)               |
| So                                             | “For Class B software, in lieu of a CMMI rating by a development organization, the project will conduct an evaluation, performed by a qualified evaluator selected by the Center Engineering Technical Authority, of the seven process areas listed in SWE-032 and mitigate any risk, if deficient. | Review (SAR)           |
| Re                                             |                                                                                                                                                                                                                                                                                                     | E-032]                 |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| Int                                            |                                                                                                                                                                                                                                                                                                     |                        |
| So                                             | This exception is intended to be used in those cases in which NASA wishes to purchase a product from the "best of class provider," but the best of class provider does not have the required CMMI rating.”                                                                                          | ent                    |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| So                                             |                                                                                                                                                                                                                                                                                                     |                        |
| Verification Matrix [SWE-050], [SWE-060]       |                                                                                                                                                                                                                                                                                                     | Product and Process QA |
| Implement Design into Software Code. [SWE-060] |                                                                                                                                                                                                                                                                                                     |                        |
| Software User Manual [SWE-115]                 |                                                                                                                                                                                                                                                                                                     |                        |
| Software Version Description [SWE-116]         |                                                                                                                                                                                                                                                                                                     |                        |



# “Falling Off The Cliff” Notes



≡ Goddard Space Flight Center

## Software Planning

Software Inventory/Classification [SWE-20]

Determine the software safety criticality [SWE-133]



## Software Safety

Develop a Software Safety plan [SWE-023], [SWE-130], [SWE-138]

Implement design requirements for safety critical software [SWE-134]



## Compliance

Provide a compliance matrix [SWE-125]

Full compliance consistent with software classification. [SWE-139]





# Classification/Inventory Process





# NPR 7150 SW Class Definitions



≡ Goddard Space Flight Center

| Classification                                                                                      | Characteristics                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Class A</b> Human Rated Software (SW) Systems                                                    | All space flight software (SW) subsystems (ground and flight) developed and/or operated by or for NASA to support human activity in space and that interact with NASA human space flight systems.                                                                                                                                                                                                                                                                |
| <b>Class B</b> Non-Human Space Rated SW Systems or Large Scale Aeronautics Vehicles                 | Flight and ground SW that must perform reliably in order to accomplish primary mission objectives. Large scale aeronautics vehicles that are NASA unique in which the SW is integral to controls.                                                                                                                                                                                                                                                                |
| <b>Class C</b> Mission Support SW or Aeronautics Vehicles or Major Engineering Research Facility SW | Flight/ground SW necessary for the science return from a single (non-critical) instrument or is used to analyze/process mission data or other SW for which a defect could adversely impact attainment of any secondary mission objectives or cause operational problems for which potential workarounds exist. Systems for non-large scale aeronautics vehicles in which SW is integral to controls. Systems that operate a major engineering/research facility. |



# NASA Software Class Examples



≡ Goddard Space Flight Center

## Class A Software

- Human Rated Software
- Human and Vehicle Health & Safety



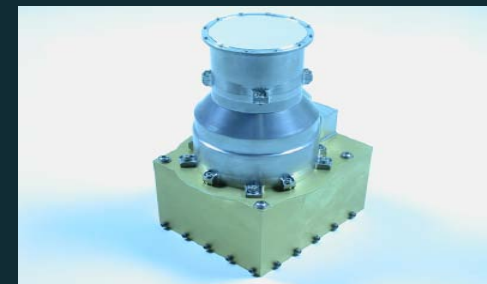
## Class B Software

- Spacecraft Flight SW
- Primary Instrument SW
- Ground SW



## Class C Software

- Non-primary Instrument Flight SW
- Spacecraft Simulators
- Large Scale Facilities Operations/Control (control of high-value assets)
- GSE that interfaces to flight hardware



**Criticality, Complexity, Reliability, Safety**

# Safety Criticality





# Safety Critical Software



≡ Goddard Space Flight Center

The NASA Software Safety Standard, NASA-STD-8719.13C, describes safety critical software as software that:

- Controls or mitigates system hazards
- Resides on the same processor as safety critical software and is not logically separated
- Processes data that drives safety decisions
- Provides V&V of safety critical systems

**The Hazard Analysis and  
Reliability Analysis ( FTA/FMEA)  
are the drivers for identifying  
the critical elements**



# Safety Critical Software Design Requirements



≡ Goddard Space Flight Center

## Safety-Critical Software must:

- Initialize (and reinitialize), transition and terminates to a safe state
- Validate input and output data prior to use
- Provides failure detection and correction
- Utilize two step commanding

n. Incorporate requirements in the coding methods, standards, and/or criteria to clearly identify safety-critical code and data within source code comments





# Safety Critical Software Rigor Simplified



≡ Goddard Space Flight Center

- Identify Safety Critical Software
  - Designate Safety Critical Requirements as such and mark software design elements(functions, data, etc.)
- Apply design requirements for Safety Critical Software
- If changing Safety Critical Software, the changes must be evaluated for safety considerations
- Verify the software meets the safety critical requirements
  - High fidelity testing
  - Nominal and off-nominal testing

# Compliance





# How To Evidence Compliance



≡ Goddard Space Flight Center

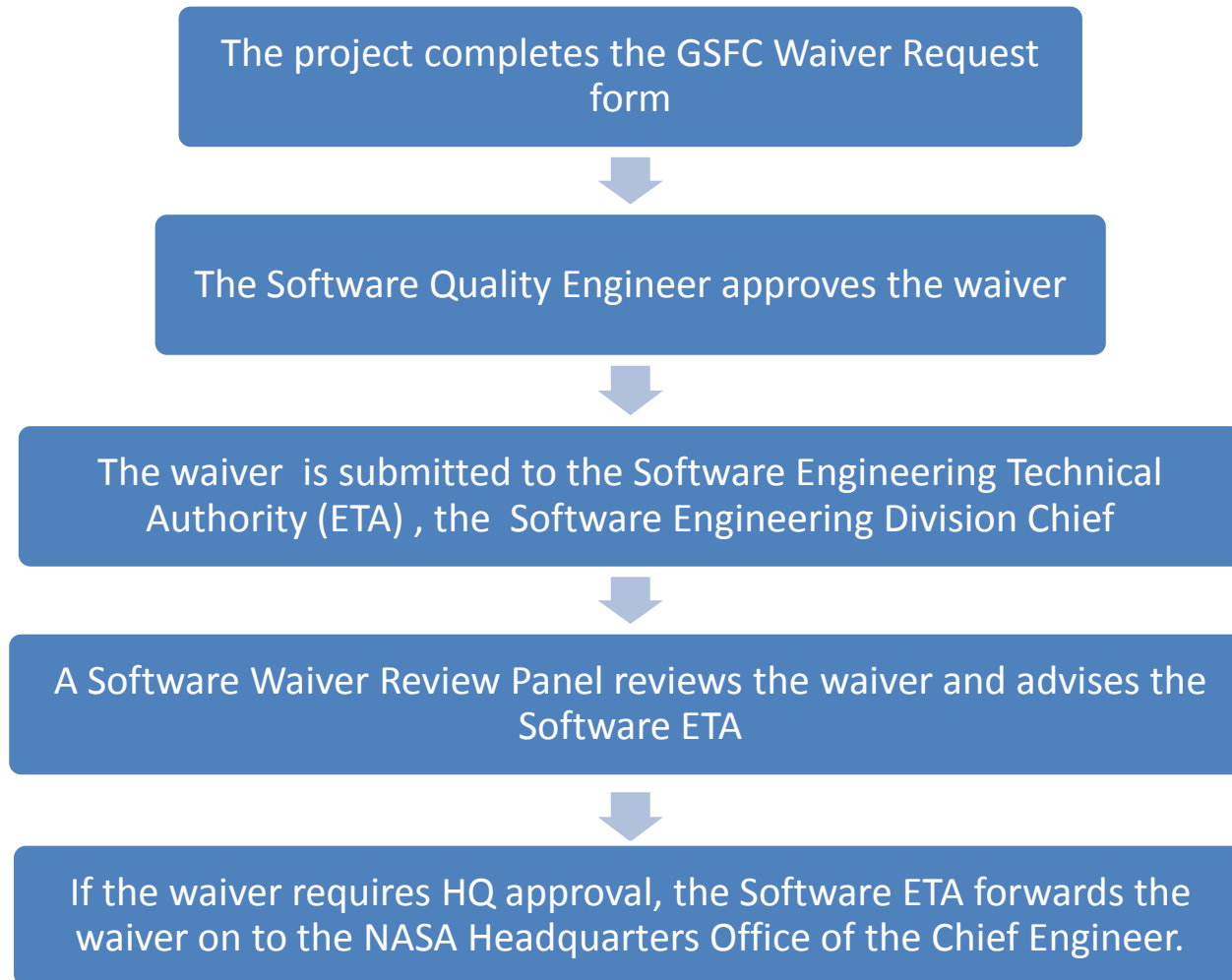
- Utilize the compliance matrix from the NPR and your software plans to derive your compliance matrix
- Be sure to identify the “auditable” artifact that is produced by your plans to show compliance
- Provide access to the CM system or repository that houses your development artifacts
- As artifacts are completed, and placed under CM, add the associated identifier to the compliance matrix



# GSFC Waiver Workflow



≡ Goddard Space Flight Center





# Waiver Approval Authority



≡ Goddard Space Flight Center

The following requirements require approval by NASA HQ:

| Requirement Number(s)              | Description                     |
|------------------------------------|---------------------------------|
| SWE-013                            | Required Software Plans         |
| SWE-020, SWE-132                   | Software Classification         |
| SWE-032                            | CMMI Requirements               |
| SWE-086                            | Risk Management Requirements    |
| SWE-022, SWE-106                   | Software Assurance Requirements |
| SWE-023, SWE-130, SWE-133, SWE-138 | Software Safety Requirements    |

# Challenges & Concerns





# Typical Supplier Concerns



≡ Goddard Space Flight Center

| Problem                                   | Solutions                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Excessive requirements for software plans | <p>Establish organizational/multi-project plans.</p> <p>Consolidate plans</p> <p>Examine your current process, to ensure that it is fully documented.</p> <p>Perform a gap analysis of your existing process against the NPR.</p> <p>Assess the gaps for risks, and modify the process accordingly, applying for waivers where an approach exist for managing the risk.</p> |



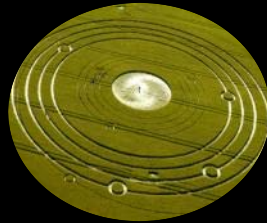
# Typical Supplier Concerns Cont.



≡ Goddard Space Flight Center

| Typical Problem                               | Solutions                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Burdensome reporting and metrics requirements | Make effective use of software tools and their reporting capabilities                                                                                                                                                                                                        |
| Cost of oversight (QA, IV&V, Supply Chain)    | <p>Review oversight plans (SAP, IPEP) for understanding of the scope of activities.</p> <p>Invite QA and IVV to participate as stakeholders or voluntary participants in your processes.</p> <p>Include receipt of and response to QA and IVV findings in your schedule.</p> |

# Final Thoughts





# Final Thoughts



≡ Goddard Space Flight Center

- 7150.2A is the NASA standard, but it is mostly comprised of standard methods employed by mature development teams.
- The cost of implementing the NPR is offset by the early identification of process inefficiencies that yield errors
- Your NASA SW Systems Engineering leads, and SW Assurance leads, have seen the NPR adopted successfully by multiple shops with varying profiles, and are available to assist you in navigating the requirements, and avoiding the risk of overcomplicating your efforts to comply with the standard

# Q&A





≡ Goddard Space Flight Center

---

Please email additional  
questions/feedback to:

[Isaac.e.mcginnis@nasa.gov](mailto:Isaac.e.mcginnis@nasa.gov)

[Manuel.d.maldonado@nasa.gov](mailto:Manuel.d.maldonado@nasa.gov)